UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,389	07/26/2001	Neil Andrew Cowie	550-251	5037

23117	7590	06/10/2005

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER
HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on <u>22 March 2005</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-96</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-96</u> is/are rejected.

7)☐ Claim(s) <u>5-14,21-30,37-46,53-62,68-78 and 85-94</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>30 October 2001</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
   application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

This action is in response to the communication filed on 3/22/2005.

DETAILED ACTION

1.   Claims 1-96 have been examined.

2.   All objections and rejections not set forth below have been withdrawn.

Title

3.   The title of the invention is acceptable.

Priority

4.   No claim for priority has been made for this application.

5.   The effective filing date for the subject matter defined in the pending claims in this

application is 07/26/2001.

Information Disclosure Statement

6.   The information disclosure statement (IDS) submitted on 7/30/2002 is in compliance

with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information

disclosure statement.

Drawings

7.   The drawings filed on 10/30/2001 are acceptable for examination proceedings.

Claim Objections

8.   Claims 5-14, 21-30, 37-46, 53-62, 68-78, and 85-94 are objected to failing to comply

with proper numbering.

9.   The applicant is reminded that a series of singular dependent claims is permissible in

which a dependent claim refers to a preceding claim which, in turn, refers to another preceding

claim.

A claim which depends from a dependent claim should not be separated by any claim

which does not also depend from said dependent claim. It should be kept in mind that a

dependent claim may refer to any preceding independent claim. In general, applicant's sequence

will not be changed. See MPEP § 608.01(n).

As noted by the applicants in the response filed 3/22/2005, the claim numbering does not

need to be changed in response to this objection.

Claim Rejections - 35 USC § 102

10.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11.   Claims 1-3, 5, 17-19, 21, 33-35, 37, 49-51, 53, 65-67, 69, 81-83, and 85 are rejected

under 35 U.S.C. 102(b) as being anticipated by Cozza (US Patent Number 5,649,095).

12.   Regarding claims 1, 17, 33, 49, 65, and 81, Cozza disclosed a system, method, and

computer program product (See Cozza Claims and Col. 1 Lines 26-33) comprising a computer

program operable to control a computer to detect a known computer program within a packed

computer file, said packed computer file being unpacked upon execution, said computer program

comprising (See Cozza Abstract and Col. 3 Paragraph 6: resource data reading logic for reading

resource data within said packed computer file (See Cozza Col. 6 Lines 21-23 and 29-34), said

resource data specifying program resource items used by said known computer program (See

Cozza Col. 2 Paragraph 7) and readable by a computer operating system without dependence

upon which unpacking algorithm is used by said packed computer file (See Cozza Col. 6

Paragraphs 2-3 wherein the compressed file is not decompressed in order to read the resource

forks information); and resource data comparing logic for generating characteristics of said

resource data (See Cozza Paragraph 1 Lines 58-65 wherein it was inherent that the characteristic

data was generated in order for the data to have been compared) and for comparing said

characteristics of said resource data with characteristics of resource data of said known computer

program (See Cozza Col. 7 Lines 35-39 and Col. 1 Lines 58-65) and for detecting a match with

said known computer program indicative of said packed computer file containing said known

computer program (See Cozza Col. 7 Lines 35-39 and Col. 1 Lines 58-65).

13.   Regarding claims 2, 18, 34, 50, 66, and 82, Cozza disclosed that said known computer

program is one of: a Trojan computer program; and a worm computer program (See Col. 1 Lines

22-32 and Col. 7 Lines 35-39).

14.   Regarding claims 3, 19, 35, 51, 67, and 83, Cozza disclosed that said resource data

comparing logic is operable to compare said resource data with characteristics of a plurality of

known computer programs to detect if said packed computer program contains one of said

plurality of known computer programs (See Cozza Col. 7 Lines 35-40).

15.   Regarding claims 5, 21, 37, 53, 69, and 85, Cozza disclosed that said program resource

items used by said known computer program include one or more of: icon data; string data;

dialog data; bitmap data; menu data; and language data (See Cozza Col. 2 Paragraph 7).

Claim Rejections - 35 USC § 103

16.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or*
> *described as set forth in section 102 of this title, if the differences between the subject*
> *matter sought to be patented and the prior art are such that the subject matter as a whole*
> *would have been obvious at the time the invention was made to a person having ordinary*
> *skill in the art to which said subject matter pertains. Patentability shall not be negatived*
> *by the manner in which the invention was made.*

17.   Claims 4, 9-11, 13-14, 20, 25-27, 29-30, 36, 41-43, 45-46, 52, 57-59, 61-62, 68, 73-75,

77-78, 84, 89-91, and 93-94 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Cozza as applied to claims 1, 17, 33, 49, 65, and 81 above respectively, and further in view of

Hyppönen et al. (US Patent Number 6,577,920) hereinafter referred to as Hypponen.

18.   Regarding claims 4, 20, 36, 52, 68, and 84, Cozza disclosed comparing the resource data

with resource data of a known program (See Col. 1 Lines 58-65, Col. 6 Paragraph 3 and Col. 7

Lines 35-40), but Cozza failed to specifically disclose using program fingerprint data for the

comparison.

Hypponen teaches a method of virus scanning in which signatures (fingerprint) of a file

are created and compared to signatures of known infected files in order to detect viruses (See

Hypponen Col. 3 Lines 14-25).

It would have been obvious to the ordinary person skilled in the art at the time of

invention to employ the teachings of Hypponen in the virus scanning of Cozza by creating a

signature of the resources of the compressed file and comparing it to previous signatures. This

would have been obvious because the ordinary person skilled in the art would have been

motivated to scan the files as quickly as possible, without compromising security.

19.   Regarding claims 9, 25, 41, 57, 73, and 89, the combination of Cozza and Hypponen

disclosed the fingerprint data including a checksum (See Hypponen Col. 4 Lines 55-59) value

calculated in dependence upon one or more of: a number of program resource items specified

beneath each node within hierarchically arranged resource data; string names associated with

program resource items within said resource data; and sizes of program resource items within

said resource data (See Cozza Col. 5 Lines 1-9 wherein it would have been inherent that the size,

or amount of data, the string names in the data, and the number of the resource items in that data

would have effected the calculation of the checksum).

20.   Regarding claims 14, 30, 46, 62, 78, and 94, Cozza and Hypponen disclosed the

checksum being SHA, which shifts after each operation (See Hypponen Col. 4 Lines 56-59).

21.   Regarding claims 10, 26, 42, 58, 74, and 90, the combination of Cozza and Hypponen

disclosed the signature including multiple resource items (See Cozza Col. 1 Lines 63-65 and Col.

2 Paragraph 7).

22.   Regarding claims 11, 27, 43, 59, 75 and 91, the combination of Cozza and Hypponen

disclosed that said fingerprint data includes a location within said resource data of an entry

specifying a program resource item having a largest size (See Cozza Col. 6 Lines 29-45).

23.   Regarding claims 13, 29, 45, 61, 77,and 93, the combination of Cozza and Hypponen

disclosed that said fingerprint data includes a flag indicating which data is included within said

fingerprint data (See Cozza Col. 5 Paragraph 3).

24.   Claims 12, 28, 44, 60, 76, and 92 are rejected under 35 U.S.C. 103(a) as being

unpatentable over the combination of Cozza and Hypponen as applied to claims 4, 20, 36, 52, 68,

and 84 above respectively, and further in view of Hodges et al. (US Patent Number 6,269,456)

hereinafter referred to as Hodges.

The combination of Cozza and Hypponen disclosed creating fingerprint data for detecting

viruses (See rejection of claim 4 above), but failed to disclose providing a time of compilation in

the fingerprint data.

Hodges teaches that in a virus protection system, virus signature files can be

automatically updated with new signatures when necessary, if a latest revision time is provided

with the files (See Hodges Col. 2 Paragraph 6 and Col. 4 Paragraph 6).

It would have been obvious to the ordinary person skilled in the art at the time of

invention to employ the teachings of Hodges in the virus scanning system of Cozza and

Hypponen by providing a time of revision with each signature. This would have been obvious

because the ordinary person skilled in the art would have been motivated to ensure that the

system was protected against the most recently discovered viruses.

25.   Claims 6-8, 15-16, 22-24, 31-32, 38-40, 47-48, 54-56, 63-64, 70-72, 79-80, 86-88, and

95-96 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cozza as applied to claims

1, 17, 33, 49, 65, and 81 above, and further in view of Pietrek ("Peering Inside the PE: A Tour of

the Win 32 Portable Executable").

Regarding claims 16, 32, 48, 64, 80, and 96, Cozza disclosed detecting a known

computer program in a compressed computer file, the file including resource data (See rejection

of claim 1 above), but failed to specifically name the Win32 PE file as one of these files.

Pietrek teaches that a Win32 PE file is an executable file which contains un-initialized code and resources, which when executed the code is initialized using the resources (See Pietrek Page 21 PE File Base Relocations).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Pietrek in the virus detector of Cozza by allowing the scanning of Win32 PE files and their resources. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against Win32 PE files containing viruses.

Regarding claims 6-8, 22-24, 38-40, 54-56, 70-72, and 86-88, the combination of Cozza and Pietrek disclosed specifying a storage location for each resource item as an offset, and the size of each resource (See Pietrek Page 20 Table 13 Offsets and Page 21 Fig. 14 DWORD OffsetToData).

Regarding claims 15, 31, 47, 63, 79, and 95, Cozza and Pietrek disclosed decompressing the computer program upon execution (See Pietrek Page 21 PE File Base Relocations).

Response to Arguments

26.   Applicants' arguments filed 3/22/2005 have been fully considered but they are not persuasive. Applicants argue primarily that:

      i.   Cozza did not disclose "without dependence upon...packed computer file".

      ii.   Cozza did not disclose generating characteristics without unpacking the files or with knowing the unpacking algorithm.

         iii.   Cozza did not disclose reading resource data with said packed computer

file.

         iv.   Cozza teaches that one must know the compression algorithm in order to

obtain the size information from the decompressed file.

27.   Regarding applicants' argument i. that Cozza did not disclose "without dependence

upon...packed computer file", the examiner has considered the argument and does not find it

persuasive. Cozza did not disclose that the file must be decompressed and therefore it was not

dependant on the compression algorithm (See Cozza Col. 6 Lines 18-20 wherein Cozza clearly

states that the file could be decompressed, or opened, or special code could be executed.)

Therefore, the examiner does not find the argument persuasive.

28.   Regarding applicants' argument ii., that Cozza did not disclose generating characteristics

without unpacking the files or without knowing the unpacking algorithm, the examiner has

considered the argument and does not find the argument persuasive. In response to applicants'

argument that the references fail to show certain features of applicant's invention, it is noted that

the features upon which applicant relies (i.e., "without unpacking the files or without knowing

the unpacking algorithm) are not recited in the rejected claim(s). Although the claims are

interpreted in light of the specification, limitations from the specification are not read into the

claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Therefore, the

examiner does not find the argument persuasive and will not address this argument further.

29.   Regarding applicants' argument iii., that Cozza did not disclose reading resource data

within said packed computer file, the examiner has considered the argument and does not find

the argument persuasive. In Col. 6 Lines 21-23 and 29-34, Cozza clearly disclosed reading the

fork size from the cache information. The fork size constitutes "resource data within the packed computer file". Therefore, the examiner does not find the argument persuasive.

30.   Regarding applicants' argument iv., that Cozza teaches that one must know the compression algorithm in order to obtain the size information from the decompressed file, the examiner has considered the argument and does not find the argument persuasive. Firstly, the applicants fail to show where this so called disclosure is located in Cozza. Lines 18-20 of Col. 6 of Cozza clearly show that the system of Cozza does not require decompression to read the resource data. The applicants have misinterpreted the cited portion to have read "This involves decompressing the file, opening the file, and executing some special…code in order to obtain this information." In fact Cozza disclosed in the cited portion that obtaining the information could involve decompressing, opening, or executing. As such, decompression was not required and no knowledge of the algorithm in required as well. Therefore, the examiner does not find the argument persuasive.

31.   As such, because these arguments were the only arguments presented for all the claims, and because the examiner does not find the arguments persuasive, the examiner has maintained the rejections presented above and in the previous action dated 12/22/2004.

Conclusion

32.   Claims 1-96 have been rejected.

33.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

     a.   Arnold et al. (US Patent Number 5,440,723) disclosed a method for creating virus signatures and using the signatures to detect viruses.

    b.   Cozza (US patent Number 5,473,769) disclosed a method for scanning for viruses

involving scanning the resource fork of a file.

    c.   Beetz (GB 2365158) disclosed a method for detecting viruses contained in a

compressed executable.

34.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

35.   A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

36.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790.

The examiner can normally be reached on M-F 8-4.

    If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
6/6/2005

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER